

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*
 1878 Sunset Avenue, Apt. 82, Cincinnati, OH 45238

Case No. **1:23-MJ-00957**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A-9 (incorporated by reference).

located in the _____ Southern _____ District of _____ Ohio _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B (incorporated by reference).

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. 1028(a)(7), 1028(f), 1028A, 922(a)(6), 371	Identity Theft, Identity Theft Conspiracy, Aggravated Identity Theft, False Statement During Purchase of a Firearm, Conspiracy to Commit an Offense Against the United States

The application is based on these facts:

See Attached Affidavit (incorporated by reference).

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days *(give exact ending date if more than 30 days: _____)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Derek Graham

Applicant's signature

Derek Graham, Special Agent, ATF

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
 _____ FaceTime Video Conference *(specify reliable electronic means)*.

Date: **Nov 16, 2023**

Stephanie K. Bowman

Judge's signature



City and state: Cincinnati, Ohio

Hon. Stephanie K. Bowman, U.S. Magistrate Judge

Printed name and title

Attachment A-9

The property to be searched, **SUBJECT PREMISES – SUNSET AVENUE** is located at 1878 Sunset Avenue, Apartment 82, Cincinnati, OH 45238. The property to be searched is an apartment within a multi-family apartment building constructed of brick with glass entry doors. The numbers “82” appear on the center of a red door of the apartment. The premises to be searched includes the apartment home and all associated storage areas on the property, including but not limited to garages, sheds, cellars, and other containers.



ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. §§ 1028(a)(7) (Identity Theft), 1028(f) (Identity Theft Conspiracy), 1028A (Aggravated Identity Theft), 922(a)(6) (False Statement During Purchase of a Firearm), and 371 (Conspiracy) (collectively, the “Target Offenses”), those violations involving MARKENDRA CARTER, TEAGUE JACKSON, EDWARD WASHINGTON, ZACHARY HARRIS, and other known and unknown coconspirators and occurring after on or about September 1, 2023, including:

- a. Records and information relating to the purchase, attempted purchase, acquisition, possession, sale, and/or transfer of firearms, ammunition, and/or firearms accessories;
- b. Records and information relating to the possession, theft, use, and/or transfer of personally identifiable information and financial information, including but not limited to credit card information;
- c. Records and information relating to the making of false statements during the purchase of a firearm;
- d. Records and information relating to the identity of coconspirators to the Target Offenses;
- e. Records and information relating to preparatory steps taken in furtherance of the Target Offenses;
- f. Records and information relating to steps taken to evade capture for the Target Offenses;

- g. Records and information relating to communications between any coconspirators involved in the Target Offenses;
 - h. Records and information relating to the proceeds of the Target Offenses, including but not limited to information about financial accounts used to receive, possess, store, and transfer criminal proceeds;
 - i. Records and information relating to occupancy at, and/or control over, a premises or vehicle, including but not limited to rental agreements and records, leases, mail, vehicle registrations, utility bills and receipts, and personal identification and photographs.
2. Firearms, ammunition, holsters, gun cases, gun boxes, and other firearms accessories.
3. Copies of ATF Forms 4473s, and any related purchase and sale documents and receipts.
4. Any U.S. currency in an amount of at least \$100 that constitutes evidence of, or the proceeds of, illegal firearm sales.
5. Keys, key fobs, garage door openers, and other items that can be used to access a vehicle or premises.
6. Financial instruments used in furtherance of violations of the Target Offenses, or that constitute proceeds of violations of the Target Offenses, including but not limited to credit cards, debit cards, prepaid cards, money orders, and cashier's checks.
7. Computers or storage media used as a means to commit the violations described above.

8. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;

- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of the Premises described in Attachments A-1 through A-9, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of a device found at the premises, to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF
THE NINE LOCATIONS DESCRIBED IN
ATTACHMENTS A-1 THROUGH A-9

Case No. 1:23-MJ-00957

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Derek Graham, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of applications under [Federal Rule of Criminal Procedure 41](#) for warrants to search the premises listed below, further described in Attachments A-1 through A-9, for the things described in Attachment B:

- The person of **MARKENDRA CARTER**, DOB 05/XX/1989, SSN XXX-XX-8771 (A-1)
- The person of **ZACHARY HARRIS**, DOB 02/XX/2000, SSN XXX-XX-6606 (A-2)
- The person of **TEAGUE JACKSON**, DOB 05/XX/2001, SSN XXX-XX-1249 (A-3)
- The person of **EDWARD WASHINGTON**, DOB 09/XX/1999, SSN XXX-XX-9644 (A-4)
- The white 1997 Honda Accord bearing Ohio registration KDW1209 and VIN 1HGCD5636VA218236 (the “ACCORD”) (A-5)
- The maroon 2008 Hyundai Sonata bearing Ohio registration MZBDW and VIN 5NPET46C08H338521 (the “SONATA”) (A-6)
- The silver 2008 Pontiac G6 bearing temporary Ohio registration R018583 and VIN 1G2ZF57B384147609 (the “PONTIAC”) (A-7)
- 11467 Ravensburg Court, Cincinnati, OH 45240 (“SUBJECT PREMISES – RAVENSBURG COURT”) (A-8)
- 1878 Sunset Avenue, Cincinnati, OH 45238, Apt. 82 (“SUBJECT PREMISES – SUNSET AVENUE”) (A-9)

(collectively, the “**SUBJECT PREMISES**”).

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms & Explosives (ATF), and have been so employed since October of 2007. As a part of my training with the ATF, I graduated from the Federal Law Enforcement Training Center, Criminal Investigator School, located in Brunswick, Georgia. I graduated from the ATF Special Agent Basic Training Academy, located in Brunswick, Georgia, in April 2008. Prior to my employment with ATF, I was a Federal Air Marshal in the Department of Homeland Security from June 2006 through October 2007. In addition, I was a Criminal Research Specialist with the Washington, DC High Intensity Drug Trafficking Area/Drug Enforcement Administration from June 2003 through June 2006. I am a graduate of Augustana College, where I received a Bachelor’s degree in Business Administration in May of 2002. I am also a graduate of Boston University, where I received a Master’s degree in Criminal Justice in June of 2006.

3. I have experience in the investigation, apprehension, and prosecution of individuals suspected of being involved in federal firearms and drug offenses. I have specific experience in investigating the use of cell phones by criminal suspects who are involved in the commission of those offenses. I have been trained by ATF as a Digital Media Collection Specialist (DMCS) and have completed more than 285 forensic extractions of cellular telephones, computers, and other electronic storage media. I have also reviewed forensic extractions of cellular telephones, computers, and other electronic storage media, and have examined content and communications contained within these devices obtained by forensic extraction. This content includes records of communication through call logs, text message content, images and videos, and communication made through various social media applications.

4. I know from training and experience that individuals typically keep cell phones in their residences, on their persons, or within their immediate control, such as in the cupholder of a car they are driving, because cell phones are regularly used and possessed as an item of personal property. I also know from my training and experience that in today's age it is typical for individuals engaged in criminal activity to possess multiple active cellular phones at one time. For example, many criminals have one phone that they use for personal communications (e.g., with family members) and another phone that they use to communicate with criminal associates.

5. I also know based on my training and experience that, when individuals are involved in an illegal business, such as firearms or drug trafficking, those individuals commonly maintain in their residences, on their persons, and/or in their vehicles lists of customers, supplier lists, pay/owe sheets, receipts, address books, and other documents listing the price and quantity of items sold, as well as the date the items were purchased, possessed, and sold. These records may be stored in paper form or on electronic devices, such as cell phones and other electronic storage media.

6. Additionally, based on my training and experience, I know that firearms traffickers commonly store in their residences and/or vehicles, as well as carry on their persons, fruits and contraband of their trafficking, such as firearms, ammunition, firearms accessories, and the proceeds of their trafficking. It is also common for individuals to carry on their person or in their vehicles items allowing them to access premises they control, such as house keys and garage-door openers, as well as documentation showing their association with certain premises, such as identification cards and other paperwork listing home addresses.

7. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to

show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

8. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1028(a)(7) (Identity Theft), 1028(f) (Identity Theft Conspiracy), 1028A (Aggravated Identity Theft), 922(a)(6) (False Statement During Purchase of a Firearm), and 371 (Conspiracy) (collectively, the “Target Offenses”) have been committed by MARKENDRA CARTER, TEAGUE JACKSON, EDWARD WASHINGTON, ZACHARY HARRIS, and other known and unknown coconspirators. There is also probable cause to search the locations described in Attachments A-1 through A-9 for the evidence, instrumentalities, fruits, and contraband of these crimes further described in Attachment B.

PROBABLE CAUSE

A. Introduction

9. From on or about September 25, 2023, through on or about September 26, 2023, one or more unidentified persons made three separate online purchases, for a total of eight firearms, from Federal Firearms Licensee (FFL) Range USA. These orders were placed in the names of, and transferred to, MARKENDRA CARTER, TEAGUE JACKSON, and EDWARD WASHINGTON. Each of the purchases was made using stolen credit card information. Each of the firearms was transferred at FFL Range USA – Cincy West, located at 7266 Harrison Avenue, Cincinnati, which is located in the Southern District of Ohio.

10. At around the same time, i.e., on September 26, 2023, one or more unidentified persons made seven additional attempted online purchases, for a total of twenty-seven firearms, from Range USA. These orders were placed in the names of EDWARD WASHINGTON, [REDACTED]

██████ and “A.C.”¹ Six of the orders were to be picked up at Range USA– Cincy West, and one was to be picked up at Range USA’s Blue Ash location, which is also in the Southern District of Ohio.

11. As described below, further investigation has revealed additional evidence that CARTER, JACKSON, WASHINGTON, and another individual named ZACHARY HARRIS conspired to buy firearms with stolen credit card information and to pick up the firearms in straw purchases. I am now seeking several search warrants for these suspects’ persons and for vehicles and residences where they have likely stored evidence, instrumentalities, contraband, and fruits of their crimes.

B. On September 25, 2023, MARKENDRA CARTER, at FFL Range USA – Cincy West, completed the transfer of two firearms that had been purchased using stolen credit card information.

12. On September 25, 2023, at approximately 12:00am, an online order for two firearms was placed through the Range USA website in the name of MARKENDRA CARTER. The billing address and shipping address on the order were an address on “Shadow Court” in Morrow, OH. The email address associated with the purchaser was COINDEE11@GMAIL.COM. The purchase price of the firearms was \$1,153.44.

13. That same day, at approximately 10:50am, CARTER, at Range USA – Cincy West, completed an ATF Form 4473 for the transfer of the firearms. The firearms purchased online and transferred to CARTER are further described as follows:

- Glock, Model 40, 10mm caliber pistol, Serial No. CAKZ049
- Taurus, Model G3C, 9mm caliber pistol, Serial No. ADB972777

¹ Purchaser “A.C.” is being referred to by his/her initials. Based on the investigation, your affiant believes “A.C.” was one of the victims and that the individual placing the order online inadvertently used the real name of the cardholder, “A.C.”

14. A Range USA Asset Protection Coordinator provided me with information that the purchase of these two firearms by CARTER was subject of a credit card chargeback due to the unauthorized use of a credit card.

15. I reviewed the Range USA invoice related to this transfer and identified a potential victim as "T.R." During further review, I identified a variation of the billing address and shipping address detailed on the order as the current residence of T.R.; his/her true address was on Shadow Ridge Court, rather than "Shadow Court."

16. On October 13, 2023, I interviewed T.R. and he/she confirmed that he/she did not authorize the purchase of firearms utilizing his/her credit card, and that he/she did not know CARTER. T.R. said he/she had obtained the credit card from the Bass Pro Shop retail store in Cincinnati, OH on or about September 11, 2023.

17. The Range USA Asset Protection Coordinator also provided me with interior and exterior surveillance video documenting the transfer of firearms to CARTER. Interior surveillance video shows CARTER using a device that appears to be a cellular telephone while inside Range USA. See the image below, which is a zoomed-in, cropped image from the surveillance video:



18. The surveillance video also shows the following: CARTER arrived as a passenger in a silver Pontiac sedan. (Based on the evidence I describe below, I submit that there is probable cause to believe that this vehicle was the **PONTIAC**, which I detail further below.) CARTER then exited from the front passenger seat and interacted with the unidentified driver of the vehicle. She then walked into Range USA by herself. After completing the firearm transfer, CARTER exited Range USA and walked back to the **PONTIAC** while carrying the purchased firearms. The unidentified driver exited the **PONTIAC** and opened the trunk. CARTER then placed the firearms into the trunk, entered the **PONTIAC** as the front passenger, and departed from the parking lot. See image:



C. MARKENDRA CARTER is the registered owner of a silver Pontiac sedan—the PONTIAC—matching the description of the vehicle she arrived in as a passenger on September 25, 2023.

19. On November 6, 2023, from approximately 2:00 p.m. to approximately 4:15 p.m., ATF SA John Scott observed CARTER and an unidentified Black male outside the apartment complex at 1878 Sunset Avenue, Cincinnati, OH, which, as I explain below, contains **SUBJECT PREMISES – SUNSET AVENUE** (apartment 82), and which there is probable cause to believe is CARTER's residence. SA Scott saw CARTER and the unidentified Black male exit and enter the apartment building and then enter and exit the **PONTIAC** multiple times during this approximately two-hour time period.

20. At approximately 4:15 p.m., SA Scott saw CARTER and the unidentified Black male enter the **PONTIAC** and drive away, with CARTER as a passenger.

21. About five minutes later, CPD PO Zachary Kress conducted a traffic stop of the **PONTIAC** for a traffic violation and identified the driver as Montreal Williams. Williams provided his address as 1878 Sunset Avenue, Apartment 82, Cincinnati, OH 45238 (i.e., the **SUBJECT PREMISES – SUNSET AVENUE**). PO Kress identified the passenger of the vehicle as CARTER.

22. On November 7, 2023, CPD PO Amber Bolte queried a database available to law enforcement and learned that the **PONTIAC** is registered to CARTER at 1878 Sunset Avenue, Cincinnati, OH. The registration information does not include an apartment number.

23. On November 7, 2023, at approximately 9:45 a.m., SA Scott observed the **PONTIAC** parked in the parking lot of 1878 Sunset Avenue, Cincinnati, OH. See image below:



24. I have reviewed surveillance video from Range USA – Cincy West from the date of the firearms transfer to CARTER and compared the vehicles depicted in that video and the one photographed by SA Scott on November 7, 2023. I believe the vehicle observed on both dates to be the **PONTIAC** based on appearing to be the same make, model, and color; that CARTER has been observed as the passenger in the **PONTIAC** on multiple occasions; and that the **PONTIAC** is registered in her name.

D. There is probable cause to believe that MARKENDRA CARTER lives at SUBJECT PREMISES – SUNSET AVENUE.

25. As noted, CARTER is the registered owner of the **PONTIAC** registered to 1878 Sunset Avenue, Cincinnati, OH (the apartment complex containing the **SUBJECT PREMISES – SUNSET AVENUE**); however, the registration document does not include an apartment number.

26. CARTER was observed entering and exiting the apartment building located at 1878 Sunset Avenue multiple times on November 6, 2023, and then entering and exiting the **PONTIAC**.

27. On October 13, 2023, I queried CARTER in a database that is available to law enforcement that provides personal identifying information about places of residence. I learned from this report that CARTER has been associated with 1878 Sunset Avenue, Cincinnati, OH. The report I queried did not include an apartment number.

28. Although the sources I described above did not list an apartment number, evidence from CARTER's Google account, MARKENDRAWHITE@GMAIL.COM,² shows that CARTER lives in apartment 82 (i.e., **SUBJECT PREMISES – SUNSET AVENUE**). For example, on November 2, 2023, MARKENDRAWHITE@GMAIL.COM received an email from Duke Energy that read in part, "Your bill . . . is due on Nov. 6, 2023 for service at 1878 SUN** APT 82." Similarly, on October 31, 2023, MARKENDRAWHITE@GMAIL.COM received an email from Hamilton County Human Resources thanking CARTER for her interest in employment with the county. The attachment to the email was CARTER's application, which listed her full name and an address of **SUBJECT PREMISES – SUNSET AVENUE**.

² As I describe in more detail below, an account used by ZACHARY HARRIS forwarded a receipt relating to the purchase of firearms to MARKENDRAWHITE@GMAIL.COM, and shortly thereafter MARKENDRA CARTER arrived at the FFL to pick up those firearms.

E. On September 25, 2023, TEAGUE JACKSON, at FFL Range USA – Cincy West, completed the transfer of three firearms and assorted ammunition that were purchased using stolen credit card information.

29. On September 25, 2023, at approximately 1:13pm, an online order for three firearms and assorted ammunition was placed through the Range USA website in the name of TEAGUE JACKSON. The billing address and shipping address on the order was an address on McFarran Avenue in Cheviot, OH. The email address associated with the purchaser was SOCHIEF677@GMAIL.COM. The purchase price of the firearms and ammunition was \$1,891.77.

30. Just hours later, on September 25, 2023, JACKSON arrived at Range USA – Cincy West. At approximately 3:14pm, JACKSON completed an ATF Form 4473 for the transfer of the firearms. The firearms and ammunition purchased online and transferred to JACKSON are further described as follows:

- Glock, Model 19 Gen5, 9mm caliber pistol, Serial No. CBNR553
- Glock, Model 19 Gen5, 9mm caliber pistol, Serial No. CBNR555
- Del-Ton, Inc., Model DTI-15, 5.56 caliber rifle, Serial No. DTI-S279945
- Three (3) Boxes of PMC .223 caliber ammunition
- Four (4) Boxes of 9mm caliber ammunition
- Two (2) Boxes of 10mm caliber ammunition

31. A Range USA Asset Protection Coordinator provided me with information that the purchase of the firearms and ammunition by JACKSON on September 25, 2023, had not yet been the subject of a credit card chargeback; however, they suspected it to also be fraudulent activity based on the purchasing pattern and the common use of the email address SOCHIEF677@GMAIL.COM, which I will detail further below.

32. I reviewed the Range USA invoice related to this transfer and identified a potential victim as “M.R.” During further review, I identified the billing address and shipping address detailed on the order as the current residence of M.R.

33. On October 16, 2023, I interviewed M.R. at his/her residence. M.R. said he/she did not authorize the purchase of firearms utilizing his/her credit card and he/she did not know JACKSON. M.R. said he/she had obtained the credit card from the Bass Pro Shop retail store in Cincinnati, OH about one month earlier. M.R. said he/she had been in contact with the credit card company about the fraudulent activity and a chargeback to his/her knowledge had been processed and that he/she had not incurred any financial loss.

34. Interior surveillance video from September 25, 2023, shows JACKSON using a device that appears to be a cellular telephone immediately before entering and then while inside Range USA. See image:



35. Range USA's surveillance video also shows that JACKSON arrived as the rear passenger of an unknown black SUV and then entered the store. The black SUV then departed without JACKSON. See image:



36. Approximately twenty minutes later, a white sedan arrived in the parking lot of Range USA and no one exited the vehicle. I believe this white sedan to be the **ACCORD**, which I detail further below. See the white car at the top right of this image:



37. Approximately two minutes after the **ACCORD** arrived at Range USA, JACKSON exited the store carrying the transferred firearms and ammunition and walked towards the **ACCORD**.

JACKSON then entered the rear passenger seat of the **ACCORD** with the transferred firearms and ammunition and departed from the area as a passenger.



F. On September 26, 2023, EDWARD WASHINGTON, at FFL Range USA – Cincy West, completed the transfer of three firearms that were purchased using stolen credit card information.

38. The next day, on September 26, 2023, at approximately 5:17pm, an online order for three firearms was placed through the Range USA website in the name of EDWARD WASHINGTON. The

billing address and shipping address on the order were an address on Dee Alva Dr. in Fairfield, OH. The online order was associated with email address SOCHIEF677@GMAIL.COM—i.e., the same email address used during the online purchase of firearms in the name of JACKSON the day before. The purchase price of the firearms was \$1,908.03.

39. About an hour later, at approximately 6:22pm, WASHINGTON arrived at Range USA – Cincy West and completed an ATF Form 4473 for the transfer of the firearms. The firearms purchased online and transferred to WASHINGTON are further described as follows:

- Glock, Model 19 Gen5, 9mm caliber pistol, Serial No. CAHF304
- Glock, Model 26 Gen5, 9mm caliber pistol, Serial No. AHYU056
- Glock, Model 27, .40 caliber pistol, Serial No. BXSL278

40. A Range USA Asset Protection Coordinator provided me with information that the purchase of the three firearms by WASHINGTON on September 26, 2023, was the subject of a credit card chargeback due to the unauthorized use of a credit card.

41. I reviewed the Range USA invoice related to this transfer and identified a potential victim as “A.C.” During further review, I identified the billing address and shipping address detailed on the order as the current residence of A.C.

42. On October 16, 2023, I interviewed A.C. at his/her residence and by phone. A.C. confirmed he/she did not authorize the purchase of firearms utilizing his/her credit card, and that he/she did not know WASHINGTON. A.C. said he/she had obtained the credit card from the Bass Pro Shop retail store in Cincinnati, OH approximately thirty to forty-five days earlier. In addition, A.C. said he/she was out of the country at the time of the fraudulent activity.

43. Interior surveillance video from September 26, 2023, shows WASHINGTON using a device that appears to be a cellular telephone immediately before entering, and then while inside, Range USA. See image:



44. I reviewed the exterior surveillance video documenting the time before and after the firearms transfer to WASHINGTON. The surveillance video shows WASHINGTON arrive as the driver of a maroon sedan (which is consistent in appearance with the **SONATA** registered to the address on WASHINGTON's driver's license, as I detail further below) and then enter the store. See image:



45. Approximately twenty-three minutes later, after completing the firearms transfer, WASHINGTON exited Range USA with the transferred firearms and approached the **SONATA**. WASHINGTON placed the transferred firearms items in the trunk of the **SONATA**, entered the driver's seat, and departed.

G. There is probable cause to believe that EDWARD WASHINGTON uses the SONATA.

46. On October 30, 2023, Cincinnati Police Department (CPD) Police Officer Amber Bolte queried databases available to law enforcement to identify vehicles utilized by or associated with WASHINGTON. PO Bolte identified a Hyundai Sonata, bearing Ohio registration MZBDW and VIN 5NPET46C08H338521 (i.e., the **SONATA**), registered to Belinda Washington at 1441 Yarmouth Avenue, Cincinnati, OH—the same address that is on WASHINGTON'S Ohio-issued Driver's License. Based on Belinda Washington having the same last name and residential address as WASHINGTON, I believe she is likely a family member of WASHINGTON.

47. I have queried law enforcement license plate reader databases for the Ohio registration associated with the **SONATA** and identified the **SONATA** as being parked in the area of The Spyglass Apartments, located at 1600 Thompson Heights Avenue, Cincinnati, OH, four times from May 5, 2023, through September 18, 2023.

48. On November 6, 2023, at approximately 2:00pm, I saw the **SONATA** parked in the parking lot of The Spyglass Apartments. I then saw WASHINGTON depart from the area as the driver of the **SONATA**.

49. On November 7, 2023, at approximately 9:30am, ATF Task Force Officer (TFO) Jason Wharton saw the **SONATA** parked in the parking lot of The Spyglass Apartments. Approximately two hours later, TFO Wharton saw WASHINGTON enter the **SONATA** and drive away.

50. Based on the foregoing, I submit that there is probable cause to believe that WASHINGTON maintains control over and uses the **SONATA**.

H. On September 26, 2023, from approximately 7:13pm through 7:22pm, six additional attempted online orders were made from FFL Range USA.

51. The Range USA Asset Protection Coordinator provided me with records for six additional attempted purchases of firearms and ammunition that occurred on September 26, 2023, from approximately 7:13pm through 7:22pm. Each of the attempted purchases was for the same items, with a total price of \$2,833.92, described as follows:

- Glock manufactured, Model 19 Gen5, 9mm caliber pistol
- Glock manufactured, Model 26 Gen5, 9mm caliber pistol
- Glock manufactured, Model 22 Gen5, .40 caliber pistol
- Glock manufactured, Model 27 Gen3, .40 caliber pistol
- Three Boxes of .45 caliber ammunition
- Three Boxes of 10mm caliber ammunition
- Four Boxes of 9mm caliber ammunition

52. The first five attempted orders, spanning from approximately 7:13pm through approximately 7:16pm on September 26, 2023, were made in the name EDWARD WASHINGTON, with a billing address on Hickory Grove Drive in Worthington, OH and a MasterCard credit card ending in 7550. The email address associated with these attempted purchases was SOCHIEF677@GMAIL.COM. This is same email address associated with the online purchase and transfer completed by WASHINGTON a few hours earlier, and the online purchase and transfer completed by JACKSON on September 25, 2023.

53. The sixth attempted order, occurring at approximately 7:22pm on September 26, 2023, was made in the name of “[REDACTED]” with the same billing address on Hickory Grove

Drive and the same MasterCard credit card ending in 7550 that were used during the five attempted purchases a few minutes earlier in the name of EDWARD WASHINGTON. The email address included with this attempted purchase was TEAMAN317@GMAIL.COM.

I. On October 26, 2023, Google identified additional email addresses linked to those used on the fraudulent purchases.

54. On October 25, 2023, a federal search warrant (Case No. 1:23-MJ-865, S.D. Ohio) was issued to search information related to Google accounts COINDEE11@GMAIL.COM, SOCHIEF677@GMAIL.COM, and TEAMAN317@GMAIL.COM—the three Google accounts linked to the purchases described above.

55. Google provided records the next day. Records related to the COINDEE11@GMAIL.COM account, which was associated with online purchases in the name of MARKENDRA CARTER, showed that it was created on September 17, 2023—just days before the fraudulent purchases described above. The subscriber information listed the user’s name as “Coin Dee.”

56. In my experience, individuals engaged in online frauds commonly create operational or “throwaway” email addresses, using false subscriber information, that they use when making a fraudulent purchase or online account. Based on the short time between when this account was created and when it was used to make the fraudulent purchases, as well as the other evidence described above showing that the purchases were made in the names of other suspects (not in the name of “Coin Dee”), I believe COINDEE11@GMAIL.COM is likely an operational account, rather than a personal account used by one of the suspects.

57. Google records also showed that the email addresses 22REALENT@GMAIL.COM and SOCHIEF677@GMAIL.COM were in a file titled:

“coindee11@gmail.com.359938183667.GoogleAccountTargetAssociation.LinkedByCookies_001.”

Based on my training and experience and knowledge of Google’s services and records, I believe that this

file lists any accounts to which the targeted Google account is linked by cookies. I know from training, experience, and from reviewing Google's Privacy & Terms, that "[c]ookies are small pieces of text sent to your browser by a website you visit. They help that website remember information about your visit, which can both make it easier to visit the site again and make the site more useful to you."³ In my experience, when two accounts are linked by cookies, that tends to show that the accounts were accessed from the same electronic device, which may be evidence that the accounts are controlled by the same user. One of the email addresses linked to COINDEE11@GMAIL.COM was new: 22REALMENT@GMAIL.COM; the other, SOCHIEF677@GMAIL.COM, was previously identified in this investigation as being associated with online purchases in the names of TEAGUE JACKSON and EDWARD WASHINGTON.

58. Records related to the SOCHIEF677@GMAIL.COM account, which was associated with online purchases in the name of JACKSON and WASHINGTON, showed that it was subscribed in the name of "So Chief," that it had been created in April 2023, and that it was linked by cookies to the email addresses OFFICIALBIGZACK1@GMAIL.COM, BIGZAC5T@GMAIL.COM, ZEBOGOTIT@GMAIL.COM, MONEYDUDE000000@GMAIL.COM, and COINDEE11@GMAIL.COM (with the last of these, as noted above, being associated with an online purchase in the name of MARKENDRA CARTER).

J. Range USA identified one of the identified email addresses as being linked to purchases by ZACHARY HARRIS.

59. I requested information from Range USA about whether any of the email addresses described above were linked to purchases in their system. On October 30, 2023, Range USA provided

³ <https://policies.google.com/technologies/cookies?hl=en-US>

information showing that BIGZAC5T@GMAIL.COM was linked to several purchases at Range USA's Cincy West and Blue Ash locations and to range-membership payments, all under the name ZACHARY HARRIS.

60. On October 30, 2023, I reviewed criminal history records for HARRIS and found that he had a 2022 charge for Theft of Credit Card.

61. Over the last approximately 18 months, I have investigated multiple schemes in which one or more individuals has purchased firearms in the name of a third party, and using stolen credit cards, and then has instructed the third party to pick up the firearms for him at Cincinnati-area FFLs. In one recent scheme, for example, the person placing the online orders used stolen credit cards to buy multiple firearms and then instructed other individuals to pick the firearms up in so-called "straw purchases" (i.e., purchases in which the person picking up the firearm is actually doing so for someone else, and therefore makes a false statement on ATF Form 4473 about the true purchasers of the firearm). In that other recent case, the person placing the online orders permitted the straw purchaser to keep one of the firearms as payment for their services.

62. In this case, the fact that none of the online orders using the stolen credit card information were in the name of ZACHARY HARRIS, but that the email addresses were linked to him—together with the pattern I have seen in multiple other recent investigations—suggests that one or more of the firearms ultimately ended up with HARRIS, and therefore that one or more of the people picking up the firearms described above was doing so as part of a straw purchase.

K. The Google records showed that COINDEE11@GMAIL.COM forwarded an email about the Range USA order to an account likely used by CARTER.

63. Records from Google show that COINDEE11@GMAIL.COM received a purchase confirmation email from Range USA dated September 25, 2023, at approximately 12:03am, for Order

No. 2124475. The items in this order are the same as those previously detailed as being purchased in the name of MARKENDRA CARTER, and this is the same Order No. that Range USA provided.

64. On the same day, at approximately 9:18am, the COINDEE11@GMAIL.COM account received an email from Range USA indicating the order was ready for pickup.

65. About 20 minutes later, at approximately 9:39am, the COINDEE11@GMAIL.COM account forwarded that email to MARKENDRAWHITE@GMAIL.COM. As previously detailed, CARTER arrived at Range USA approximately one hour later and completed the transfer of the firearms that had been purchased online.

66. Based on CARTER'S possession and use of a cellular telephone while inside Range USA, and her arriving at Range USA shortly after the purchase confirmation email was forwarded to an email address including the name of "Markendra," I believe CARTER has access to and uses cellular telephones, computers, and/or other electronic devices capable of electronic communication. I further submit that, because there would seem to be no reason for CARTER to forward the email to herself, and in light of the other evidence of straw purchasing described in this affidavit, there is probable cause to believe that one coconspirator (likely HARRIS, for the reasons described below) placed the order and received the confirmation email at COINDEE11@GMAIL.COM and that this coconspirator then forwarded the email to CARTER, intending for her to pick up the firearms in a straw purchase.

L. The Google records also showed that HARRIS uses SOCHIEF677@GMAIL.COM and that he forwarded emails about the firearm purchases to JACKSON and WASHINGTON.

67. When I reviewed the contents of the SOCHIEF677@GMAIL.COM account, I found many emails showing that the user had bought items such as fast food and shoes for shipment to **SUBJECT PREMISES – RAVENSBURG CT.**, which, as I describe below, is HARRIS's residence. Based on my training and experience, individuals involved in identity theft commonly order items online

using stolen credit cards and have the items delivered to their home addresses. Based on that experience and the other evidence in this affidavit that HARRIS is involved in identity theft and straw purchasing, I believe that SOCHIEF677@GMAIL.COM is used by HARRIS.

68. Records from Google also show that on September 25, 2023, at approximately 1:15pm, SOCHIEF677@GMAIL.COM received a purchase confirmation email from Range USA for Order No. 2126526. The items in this order were the same as those previously detailed as being purchased in the name of TEAGUE JACKSON. Approximately forty-five minutes later, this email was forwarded to JACKSONTEAGUE7@GMAIL.COM. As previously detailed, on the same day at approximately 3:14pm, JACKSON arrived at Range USA and completed the transfer of the firearms and ammunition that had been purchased online.

69. On September 26, 2023, at approximately 5:18pm, SOCHIEF677@GMAIL.COM received a purchase confirmation email from Range USA for Order No. 2129604. The items in this order were the same as those previously detailed as being purchased in the name of EDWARD WASHINGTON. Approximately ten minutes later an email was sent from Range USA to SOCHIEF677@GMAIL.COM indicating the purchased firearms were ready to be picked up. Approximately four minutes later, that email was forwarded from SOCHIEF677@GMAIL.COM to EDWARDSAVAGX@GMAIL.COM. As previously detailed, on the same date at approximately 6:22pm, EDWARD WASHINGTON arrived at Range USA and completed the transfer of the firearms that had been purchased online.

70. Based on the surveillance video showing that both JACKSON and EDWARD WASHINGTON had cell phones while inside Range USA, as well as their arriving at Range USA shortly after a purchase confirmation email was forwarded to an email address containing a variation of each of their names, I believe JACKSON and WASHINGTON have access to and use cellular

telephones, computers, and/or other electronic devices capable of electronic communication. I further submit that, as with the email forwarded to CARTER, these emails being forwarded from an account used by HARRIS to accounts appearing to be used by WASHINGTON and JACKSON is evidence that the three men are involved in a straw-purchasing conspiracy.

M. ZACHARY HARRIS is the registered owner of a white Honda sedan—the ACCORD—matching the description of the vehicle involved with the transfer of firearms to TEAGUE JACKSON.

71. On October 30, 2023, I reviewed Ohio BMV records for vehicles registered to ZACHARY HARRIS and found that he is the registered owner of a 1997 Honda Accord bearing Ohio registration KDW1209 (the “**ACCORD**”). On the same date, PO Bolte queried the **ACCORD** in a license plate reader (LPR) camera database available to law enforcement and found that the **ACCORD** had been documented by a LPR camera as recently as October 16, 2023. See image:



72. Note that this vehicle appears to have a small spoiler on the trunk lid, and a black trim piece at approximately the middle of the doors.

73. PO Bolte and I compared characteristics of the **ACCORD** with the white sedan that arrived at Range USA, which TEAGUE JACKSON later entered as a passenger after the purchase and then drove away in on September 25, 2023. As shown below, the white sedan in the video from September 25, 2023, appears to have similar trim and a similar spoiler:




74.

75. Based on the similar characteristics of the vehicle, and that the registered owner, ZACHARY HARRIS, has also been identified as being involved in the scheme to purchase firearms online and then have them transferred in person to other individuals at Range USA, I submit that there is probable cause to believe that the **ACCORD** is the vehicle used to pick up TEAGUE JACKSON after the firearms sale described above.

N. On October 28, 2023, ZACHARY HARRIS drove the ACCORD to Target World.

76. On October 31, 2023, FFL Target World provided me with a Training Class Attendance Roster. The document included identifying information, including telephone number 513-514-3151 and email address BIGZAC5T@GMAIL.COM, that HARRIS appears to have provided when he attended a training on October 28, 2023.

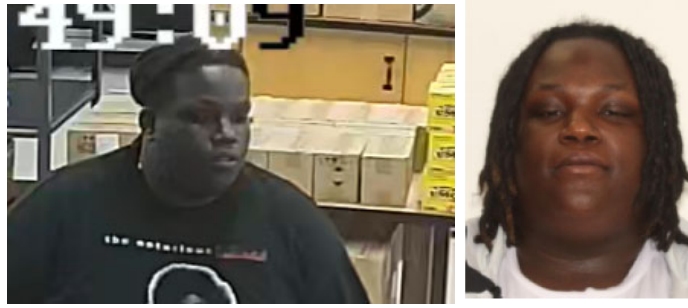
		2300 E. Kemper Road Cincinnati, OH 45241 (513) 772-3343 www.targetworld.net	
Training Class Attendance Roster			
Course: <u>CCW</u>	Date: <u>10/28/2023</u>	Instructor(s): <u>CEANEK</u>	
Please PRINT the following information clearly. (This information will not be shared with anyone outside Target World.)			

Zachary Harris	Harris	513 514 3151	Bigzac5t@gmail.com
----------------	--------	--------------	--------------------

77. Target World also provided me with interior and exterior surveillance video from when HARRIS was at Target World on October 28, 2023, which showed HARRIS arrive as the driver of the **ACCORD** and then walk inside Target World.



78. I also reviewed the interior surveillance video and saw HARRIS interacting with Target World employees. Based on a comparison with HARRIS's Ohio-issued Driver's License photo (at right below), and I believe the surveillance video shows HARRIS. The Ohio driver's license records also describe Harris as being twenty-three years old and weighing 295 pounds, which appears generally consistent with the appearance of the person captured on surveillance:



O. There is probable cause to believe that ZACHARY HARRIS resides at SUBJECT PREMISES – RAVENSBURG COURT.

79. HARRIS's Ohio issue Driver's License lists a residential address of 11467 Ravensburg Court, Cincinnati, OH (**SUBJECT PREMISES – RAVENSBURG COURT**)

80. On October 31, 2023, at approximately 10:30am, and on November 6, 2023, at about 10:00am, I saw the **ACCORD**—which, as described above, is registered in HARRIS's name, and which he drove to Target World on October 28, 2023—parked in the cul-de-sac across the street from the **SUBJECT PREMISES – RAVENSBURG COURT**.

81. On October 31, 2023, at approximately 2:30pm, I saw the **ACCORD** parked in the driveway of the **SUBJECT PREMISES – RAVENSBURG COURT**.

82. On November 13, 2023, at approximately 2:50 p.m., CPD PO Thomas Chiappone saw the **ACCORD** parked in the driveway of the **SUBJECT PREMISES – RAVENSBURG COURT**.

83. As noted above, records from Google show that SOCHIEF677@GMAIL.COM—one of the email addresses that, as described above, was used to place the online orders for firearms—received many emails with a shipping address of **SUBJECT PREMISES – RAVENSBURG COURT**. For example, on August 25, 2023, the account received an email from Donatos confirming that food would be delivered to **SUBJECT PREMISES – RAVENSBURG COURT**.

84. As another example, on September 18, 2023, SOCHIEF677@GMAIL.COM received an order confirmation email from ADMIN@LIOMUI.COM for the purchase of a pair of Balenciaga Shoes

for \$240.00. This order was placed in the name of “[REDACTED]” and listed the **SUBJECT PREMISES – RAVENSBURG COURT** as the purchaser’s address.

85. That same day, September 18, 2023, SOCHIEF677@GMAIL.COM also received a payment confirmation email from SERVICE@PAYPAL.COM. This email included **SUBJECT PREMISES – RAVENSBURG COURT** as the shipping address and the delivery name of “[REDACTED]”. The “Payment From” section of this email included the name of M.R., the same victim identified as the cardholder related to firearms transferred to TEAGUE WASHINGTON.

86. As another example, on October 10, 2023, SOCHIEF677@GMAIL.COM received an order confirmation email from RELOADEDWORLDTOUR@GMAIL.COM. This email included **SUBJECT PREMISES – RAVENSBURG COURT** as the shipping address and the delivery name of “[REDACTED]”. The billing name was “J.T.” and the billing address was on Black Squirrel Trail in Hamilton, OH.⁴ In my experience, it is common for individuals involved in identity theft crimes to use the victim’s true address as the billing address (so that it matches the credit card information) but to use their own address for the shipping address.

87. I also saw a few emails in the SOCHIEF677@GMAIL.COM account that listed a variation of the **SUBJECT PREMISES – RAVENSBURG COURT** address—namely, 11461 Ravensburg Court. Based on surveillance and my review of Google Maps, this is the residence immediately next to **SUBJECT PREMISES – RAVENSBURG COURT**. Based on my experience investigating identity theft crimes, I know that perpetrators sometimes use other addresses to receive

⁴ On November 1, 2023, I interviewed J.T., and he/she initially said he/she was not aware of any fraudulent charges utilizing his/her credit card. J.T. said he/she had obtained the credit card a couple of months earlier and used it to purchase a pair of boots from Bass Pro Shops in Cincinnati, OH. J.T. described the associate that helped him/her apply for the credit card as a heavyset Black male, which is consistent with HARRIS’s appearance. J.T. later called me again and said that, after speaking with his/her credit card company, Capital One, he/she had learned there had been fraudulent activity on his/her credit card.

deliveries in an attempt to distance themselves from the use of the stolen credit card information; they then intercept the package at the other address. Based on the other evidence that **SUBJECT PREMISES – RAVENSBURG COURT** is HARRIS's true address, including the additional emails I describe below, as well as my experience, I believe that, for the orders at issue in these few emails, HARRIS decided to use a neighbor's address.

88. The contents of 22REALENT@GMAIL.COM—one of the email addresses linked by cookies to COINDEE@GMAIL.COM—provided additional evidence that **SUBJECT PREMISES – RAVENSBURG COURT** is HARRIS's residence. For example, there were several emails addressed to “Big Zack” (and HARRIS's first name is ZACHARY), and the account also contained two receipts from Uber: one showing a pickup at **SUBJECT PREMISES – RAVENSBURG COURT** on July 1, 2023, and the other showing a dropoff there on June 30, 2023.

89. Finally, the contents of ZEBOGOTIT@GMAIL.COM—an account linked to SOCHIEF677@GMAIL.COM by cookies—contained additional evidence that **SUBJECT PREMISES – RAVENSBURG COURT** is HARRIS's address. Specifically, there were several emails in the account addressed to “Zack” or “Big Zack” and an email from July 15, 2023, from Planet Fitness that said “Hey Zack, congrats on joining Planet Fitness!” The email explained that “Zack's” membership agreement was attached, and the attached agreement listed the name “Zack H” and **SUBJECT PREMISES – RAVENSBURG COURT** as his home address.

90. Based on the foregoing, I respectfully submit that there is probable cause to believe that **SUBJECT PREMISES – RAVENSBURG COURT** is HARRIS'S residence.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

91. As described above and in Attachment B, this application seeks permission to search for records that might be found on each of the **SUBJECT PREMISES**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

92. *Probable cause.* I submit that if a computer or storage medium is found on any of the **SUBJECT PREMISES**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- A. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- B. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- C. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- D. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

93. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **SUBJECT PREMISES** because:

- A. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can

record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

B. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such

information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- C. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- D. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate

conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- E. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

94. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- A. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires

considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- B. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- C. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

95. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium,

that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

96. Because several people may share some of the **SUBJECT PREMISES** as a residence, and/or because more than one person may use some of the vehicles at issue, it is possible that the **SUBJECT PREMISES** will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

USE OF BIOMETRIC FEATURES

97. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to use.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a

fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the **SUBJECT PREMISES** and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the

aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

REQUEST FOR SEALING

98. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

Derek Graham

DEREK GRAHAM

Special Agent

Bureau of Alcohol, Tobacco, Firearms and
Explosives

Subscribed and sworn to before me via FaceTime videoconference on November 16, 2023.

Stephanie K. Bowman

HON. STEPHANIE K. BOWMAN
UNITED STATES MAGISTRATE JUDGE



Attachment A-9

The property to be searched, **SUBJECT PREMISES – SUNSET AVENUE** is located at 1878 Sunset Avenue, Apartment 82, Cincinnati, OH 45238. The property to be searched is an apartment within a multi-family apartment building constructed of brick with glass entry doors. The numbers “82” appear on the center of a red door of the apartment. The premises to be searched includes the apartment home and all associated storage areas on the property, including but not limited to garages, sheds, cellars, and other containers.



ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. §§ 1028(a)(7) (Identity Theft), 1028(f) (Identity Theft Conspiracy), 1028A (Aggravated Identity Theft), 922(a)(6) (False Statement During Purchase of a Firearm), and 371 (Conspiracy) (collectively, the “Target Offenses”), those violations involving MARKENDRA CARTER, TEAGUE JACKSON, EDWARD WASHINGTON, ZACHARY HARRIS, and other known and unknown coconspirators and occurring after on or about September 1, 2023, including:
 - a. Records and information relating to the purchase, attempted purchase, acquisition, possession, sale, and/or transfer of firearms, ammunition, and/or firearms accessories;
 - b. Records and information relating to the possession, theft, use, and/or transfer of personally identifiable information and financial information, including but not limited to credit card information;
 - c. Records and information relating to the making of false statements during the purchase of a firearm;
 - d. Records and information relating to the identity of coconspirators to the Target Offenses;
 - e. Records and information relating to preparatory steps taken in furtherance of the Target Offenses;
 - f. Records and information relating to steps taken to evade capture for the Target Offenses;

- g. Records and information relating to communications between any coconspirators involved in the Target Offenses;
 - h. Records and information relating to the proceeds of the Target Offenses, including but not limited to information about financial accounts used to receive, possess, store, and transfer criminal proceeds;
 - i. Records and information relating to occupancy at, and/or control over, a premises or vehicle, including but not limited to rental agreements and records, leases, mail, vehicle registrations, utility bills and receipts, and personal identification and photographs.
- 2. Firearms, ammunition, holsters, gun cases, gun boxes, and other firearms accessories.
 - 3. Copies of ATF Forms 4473s, and any related purchase and sale documents and receipts.
 - 4. Any U.S. currency in an amount of at least \$100 that constitutes evidence of, or the proceeds of, illegal firearm sales.
 - 5. Keys, key fobs, garage door openers, and other items that can be used to access a vehicle or premises.
 - 6. Financial instruments used in furtherance of violations of the Target Offenses, or that constitute proceeds of violations of the Target Offenses, including but not limited to credit cards, debit cards, prepaid cards, money orders, and cashier's checks.
 - 7. Computers or storage media used as a means to commit the violations described above.

8. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;

- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of the Premises described in Attachments A-1 through A-9, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of a device found at the premises, to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.